

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-342285

(43)Date of publication of application : 29.11.2002

(51)Int.Cl.

G06F 15/00

G06F 17/60

H04L 9/32

H04M 11/00

H04Q 7/38

(21)Application number : 2001-149920

(71)Applicant : NTT DATA CORP

(22)Date of filing : 18.05.2001

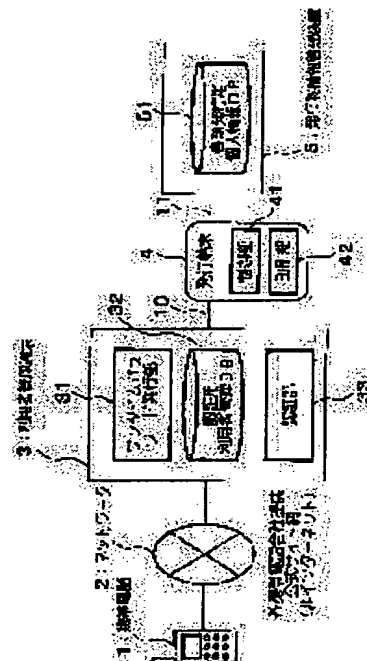
(72)Inventor : FURUTA SATOSHI

## (54) INFORMATION-ISSUING SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an information issuing system, capable of improving security, and easily collecting and issuing necessary information.

**SOLUTION:** A user management terminal 3 conducts authentication processing, based on authentication information transmitted from a portable telephone; and when the authentication is established, the user management terminal 3 issues an one-time password being information for executing authentication for receiving the permission of the issue of information to the portable telephone. Then, the issues one-time password and the identification information of the portable telephone being the target of the issue of the issued one-time password are stored to be made to correspond to each other; the identification information and one-time password issued from an issuing terminal are received; the authentication processing is executed, based on the temporarily stored information; and when the authentication is established, the issuance of the information is permitted.



## LEGAL STATUS

[Date of request for examination]

05.07.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

BEST AVAILABLE COPY

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
17/60	1 5 4	17/60	1 5 4 5 J 1 0 4
	3 0 2		3 0 2 C 5 K 0 6 7
	5 0 6		5 0 6 5 K 1 0 1
	5 1 2		5 1 2

審査請求 有 請求項の数 4 O L (全 8 頁) 最終頁に続く

(21) 出願番号 特願2001-149920 (P2001-149920)

(22) 出願日 平成13年 5 月 18 日 (2001. 5. 18)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ

東京都江東区豊洲三丁目 3 番 3 号

(72) 発明者 古田 諭

東京都江東区豊洲三丁目 3 番 3 号 株式会

社エヌ・ティ・ティ・データ内

(74) 代理人 100064908

弁理士 志賀 正武 (外 2 名)

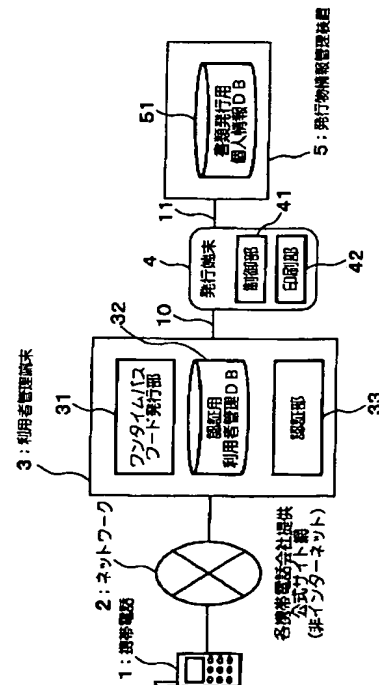
最終頁に続く

## (54) 【発明の名称】 情報発行システム

## (57) 【要約】

【課題】 セキュリティを向上させるとともに、必要な情報を簡単に取り寄せて発行することができる情報発行システムを提供する。

【解決手段】 利用者管理端末 3 は、携帯電話から送信される認証情報に基づいて認証処理を行い、認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを携帯電話に発行し、発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて一時記憶し、発行端末から送信される識別情報とワンタイムパスワードとを受信し、一時記憶された情報に基づいて認証処理を行い、認証が成立した場合に情報の発行を許可する。



#### 【特許請求の範囲】

【請求項1】 携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムであって、

前記利用者管理端末は、前記携帯電話を認証するための情報である認証情報と前記携帯電話から送信される携帯電話を識別するための情報である識別情報とを記憶する第1の記憶手段と、前記携帯電話から送信される認証情報と識別情報とを前記第1の記憶手段に記憶された情報に基づいて認証処理を行う第1の認証手段と、前記第1の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段と、前記ワンタイムパスワード発行手段によって発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報1とを対応づけて記憶する第2の記憶手段と、前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第2の記憶手段に記憶されている情報に基づいて認証処理を行う第2の認証手段と、前記第2の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段とを有し、

前記発行端末は、携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報とワンタイムパスワードとを利用者管理端末に送信する制御を行う第1の制御手段と、前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段とを有することを特徴とする情報発行システム。

【請求項2】 携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる利用者管理端末であって、

前記携帯電話を認証するための情報である認証情報と前記携帯電話から送信される携帯電話を識別するための情報である識別情報とを記憶する第1の記憶手段と、前記携帯電話から送信される認証情報と識別情報とを前記第1の記憶手段に記憶された情報に基づいて認証処理を行う第1の認証手段と、

前記第1の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段と、

前記ワンタイムパスワード発行手段によって発行された

ワンタイムパスワードと発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて記憶する第2の記憶手段と、

前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第2の記憶手段に記憶されている情報に基づいて認証処理を行う第2の認証手段と、前記第2の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段と、を有することを特徴とする利用者管理端末。

【請求項3】 前記ワンタイムパスワード発行手段は、発行毎に異なるワンタイムパスワードを発行することを特徴とする請求項2記載の利用者管理端末。

【請求項4】 携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる発行端末であって、

携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報とワンタイムパスワードとを利用者管理端末に送信する制御を行う制御手段と、

前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段と、を有することを特徴とする発行端末。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】 この発明は、携帯電話から発行が要求された情報を発行する情報発行システムに関するものである。

##### 【0002】

【従来の技術】 従来より、住民票や印鑑証明などの公的証明書が必要になった場合に、利用者は、区役所等の行政機関に出向き、必要な書類を発行してもらっている。しかし、この行政機関に出向いて必要書類を発行してもらう方法によれば、休みあるいは受け付け時間外等により行政機関が書類発行の取り扱いを行っていない場合、利用者は、即時に書類を発行してもらうことができなかった。そこで、役所、省庁などの行政機関に設けられ、発行する書類に関するデータを管理するデータベースを利用し、インターネットを介して書類の発行を行う書類発行端末を接続して書類発行を行うシステムを構築する。そして、この書類発行端末を、駅などの複数の利用者が利用可能な場所に設置し、書類発行のサービスを提供することが考えられる。

##### 【0003】

【発明が解決しようとする課題】 しかしながら、上述した書類を発行するシステムにおいては、書類発行端末を

操作することによって書類を発行することができ、悪意ある第三者によって発行端末が盗取されて書類が発行され、書類が悪用されてしまう可能性があった。本発明は、このような事情に鑑みてなされたもので、その目的は、セキュリティを向上させるとともに、必要な情報を簡単に取り寄せて発行することができる情報発行システムを提供することにある。

#### 【0004】

【課題を解決するための手段】上記目的を達成するために、本発明は、携帯電話（例えば、実施の形態における携帯電話1）から送信される情報（例えば、実施の形態における住民票、印鑑証明書などの公的証明書や有償チケットなど）の発行要求を受信する利用者管理端末（例えば、実施の形態における利用者管理端末3）と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベース（例えば、実施の形態における書類発行用個人情報データベース51）から読み出して発行する発行端末（例えば、実施の形態における発行端末4）とが接続される情報発行システム（例えば、実施の形態における情報発行システム）であって、前記利用者管理端末は、前記携帯電話を認証するための情報である認証情報（例えば、実施の形態におけるユーザIDとパスワード）と前記携帯電話から送信される携帯電話を識別するための情報である識別情報（例えば、実施の形態における電話番号、個別ID）とを記憶する第1の記憶手段（例えば、実施の形態における認証用利用者管理データベース32）と、前記携帯電話から送信される認証情報と識別情報とを前記第1の記憶手段に記憶された情報に基づいて認証処理を行う第1の認証手段（例えば、実施の形態における認証部33）と、前記第1の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段（例えば、実施の形態におけるワンタイムパスワード発行部31）と、前記ワンタイムパスワード発行手段によって発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報（例えば、実施の形態における個別ID）とを対応づけて記憶する第2の記憶手段（例えば、実施の形態における認証用利用者管理データベース32）と、前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第2の記憶手段に記憶されている情報に基づいて認証処理を行う第2の認証手段（例えば、実施の形態における認証部33）と、前記第2の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段（例えば、実施の形態における認証部33）とを有し、前記発行端末は、携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報と

ワンタイムパスワードと利用者管理端末に送信する制御を行う第1の制御手段（例えば、実施の形態における制御部41）と、前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段（例えば、実施の形態における印刷部42）とを有することを特徴とする。

【0005】また、本発明は、携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる利用者管理端末であって、前記携帯電話を認証するための情報である認証情報と前記携帯電話から送信される携帯電話を識別するための情報である識別情報とを記憶する第1の記憶手段と、前記携帯電話から送信される認証情報と識別情報とを前記第1の記憶手段に記憶された情報に基づいて認証処理を行う第1の認証手段と、前記第1の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段と、前記ワンタイムパスワード発行手段によって発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて記憶する第2の記憶手段と、前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第2の記憶手段に記憶されている情報に基づいて認証処理を行う第2の認証手段と、前記第2の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段と、を有することを特徴とする。

【0006】また、本発明は、上述の利用者管理端末において、前記ワンタイムパスワード発行手段は、発行毎に異なるワンタイムパスワードを発行することを特徴とする。

【0007】また、本発明によれば、携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる発行端末であって、携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報とワンタイムパスワードとを利用者管理端末に送信する制御を行う制御手段と、前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段と、を有することを特徴とする。

#### 【0008】

【発明の実施の形態】以下、本発明の一実施形態による

情報発行システムを図面を参照して説明する。図1は、この発明の一実施形態による情報発行システムの構成を示す概略ブロック図である。携帯電話1は、無線によってネットワーク2を介して利用者管理センタに設けられる認証用利用者管理データベース32に接続される。この携帯電話1には、携帯電話1を識別するための個別IDが予め設定されている。なお、携帯電話1は、デジタル簡易電話システムの端末であってもよい。ネットワーク2は、例えば、携帯電話1の通信サービスを提供する通信業者によって提供される公式サイト網である。ここでは、ネットワーク2としてインターネット以外のネットワークが用いられる。

【0009】利用者管理装置3は、ワンタイムパスワード発行部31と、認証用利用者管理データベース32と、認証部33とを有し、ネットワーク10を介して発行端末4に接続され、書類発行許可情報を発行端末4に送信する機能を有する。ワンタイムパスワード発行部31は、携帯電話1からの指示に応じて、ワンタイムパスワードを携帯電話1に発行する。ここでいうワンタイムパスワードとは、書類の発行許可を受けるための認証を行う情報であり、発行する毎に異なるワンタイムパスワードが発行される。また、発行されたワンタイムパスワードは、発行先のユーザID（あるいは個別ID）に対応づけられ認証用利用者管理データベース3に記憶される。

【0010】認証用利用者管理データベース32は、携帯電話1の利用者を認証するための利用者管理情報を記憶する。この認証用利用者管理データベース3に記憶される利用者管理情報の一例を図2に示す。図2に示すように、利用者管理情報には、利用者の認証を行うためのユーザIDにパスワード、利用者の住所、氏名、電話番号等、各利用者の個人の情報である個人情報、個別ID、携帯電話1の電子メールアドレス、発行したログの管理や発行した書類の管理をして証明書の真偽を確認する為に使用される情報である識別ID、ワンタイムパスワード発行部31によって発行されたワンタイムパスワードなど、が対応づけられ、記憶される。この認証用利用者管理データベース32が、上述の第1の記憶手段および第2の記憶手段に相当する。

【0011】認証部33は、携帯電話1から認証要求を受信すると、認証用利用者管理データベース32に記憶されている情報に基づいて、認証要求に含まれているパスワードと個別IDとがユーザIDに対応しているか否かを検出し、認証を行う。また、認証部33は、発行端末4から送信されるワンタイムパスワードを受信して認証用利用者管理データベース32に記憶されている利用者管理情報に基づいて認証処理を行う。さらに、認証部33は、情報の発行を許可する発行許可情報を発行端末4に発行する制御を行う。この認証部33が、上述の第1の認証手段と第2の認証手段と発行許可制御手段とに

相当する。

【0012】発行端末4は、制御部41と印刷部42とを有し、例えば、コンビニエンスストア、駅、百貨店等に設けられる。この制御部41は、携帯電話1から送信される携帯電話1を識別する識別情報（例えば、電話番号、個別IDなどのユーザが簡単に変更できない情報）とワンタイムパスワードとを受信し、受信した識別情報とワンタイムパスワードを利用者管理端末3に送信する制御を行う。また、制御部41は、利用者管理端末3から書類発行許可情報を受信した場合に、受信した書類発行許可情報を発行物情報管理装置5に送信する制御を行う。書類発行許可情報とは、発行物情報管理装置5に記憶されている情報を発行端末4に送信し、発行端末4による発行物の発行を許可する情報である。また、制御部41は、発行物を指定する情報が入力部を介して入力された場合に、発行物を指定する情報を発行物情報管理装置5に送信する。ここで、発行物を指定する情報とは、発行物情報管理装置5に記憶されている情報を指定して発行物を発行させるための情報である。

【0013】印刷部42は、制御部41からの指示に応じて印刷物の印刷を行う。また、発行端末4は、各種情報を表示するCRT（Cathode Ray Tube）または液晶表示装置等の表示部と、キーボード、マウス等の入力部と、発行物を指定する情報に基づいて料金を算出し投入部から投入される料金の精算を行う課金部とを有する。なお、この表示部と入力部とをタッチパネルなどで構成するようにしてもよい。

【0014】発行物情報管理装置5は、書類発行用個人情報データベース51を有し、専用線11によって発行端末4に接続される。書類発行用個人情報データベース51は、利用者個人に関する情報を記憶している。利用者個人に関する情報とは、例えば、利用者の住所、氏名等の個人の情報と、これら個人の情報に基づいて住民票や印鑑証明等の書類を作成して発行するための情報とが含まれる。発行物情報管理装置5は、発行端末4から発行物を指定する情報を受信した場合に、受信した発行物を指定する情報に対応する利用者個人に関する情報を書類発行用個人情報データベース51から読み出し、発行データとして発行端末4に専用線11を介して送信する。また、発行物情報管理装置5は、発行端末4からの要求に応じて、識別IDを発行する機能を有する。

【0015】次に、上述した構成における情報発行システムの動作を図面を用いて説明する。図3は、図1の構成における情報発行システムの動作を説明するための説明図である。ここでは、発行物として、住民票を発行する場合について説明する。また、ここでは、携帯電話1の利用者が発行端末4の電子メールアドレスを把握しているあるいは、携帯電話1に発行端末4の電子メールアドレスが記憶されているものとする。まず、利用者は、携帯電話1を携帯し、発行端末4が設置されている場所

に出向く。そして、携帯電話1の入力キーを操作し、ネットワーク2（公式サイト網）を介して、利用者管理端末3との通信を確立するための認証用のホームページにアクセスする。そして、このホームページの入力フォーマットに従って、ユーザIDとパスワードとを含む認証要求を入力し、ネットワーク2を介して利用者管理端末3に送信する。このとき、認証要求には、送信元を示す携帯電話1の個別IDがさらに付加されて送信される（ステップS1）。

【0016】利用者管理端末3は、携帯電話1から認証要求を受信すると、認証用利用者管理データベース32に記憶されている情報に基づいて、認証部33によって、受信した認証要求に含まれているパスワードと個別IDとがユーザIDに対応しているか否かを検出し、認証処理を行う（ステップS2）。認証処理において、パスワードと個別IDとがユーザIDに対応していない場合、利用者管理端末3は、携帯電話1にエラーを送信する。

【0017】一方、認証処理において、パスワードと個別IDとがユーザIDに対応している場合、利用者管理端末3は、ワンタイムパスワード発行部31によってワンタイムパスワードを発行し、発行したワンタイムパスワードを携帯電話1のユーザIDに対応づけて認証用利用者管理データベース32に記憶するとともに、携帯電話1に送信する（ステップS3）。このワンタイムパスワードの送信は、認証されたユーザIDとパスワードに対応づけて認証用利用者管理データベース32に記憶されている電子メールアドレスが送信先として設定されて送信される。

【0018】携帯電話1は、利用者管理端末3からワンタイムパスワードを受信すると、ワンタイムパスワードを受信したことを表示画面に表示する。このとき、ワンタイムパスワードそのものは、表示画面に表示されない。利用者は、ワンタイムパスワードを受信したことを確認した後、送信元として携帯電話1の電子メールアドレスが設定されたワンタイムパスワードと個別IDとを電子メールを発行端末4に転送する（ステップS4）。

【0019】発行端末4は、制御部41によって携帯電話1から受信したワンタイムパスワードと個別IDとを含む電子メールを利用者管理端末3に送信し、ワンタイムパスワードが正しいか否かを問い合わせ、認証依頼をする（ステップS5）。利用者管理端末3は、発行端末4から送信される電子メールを受信すると、認証用利用者管理データベース32に記憶されている情報に基づいて、電子メールに含まれる携帯電話1のワンタイムパスワードと個別IDとが対応しているか否かを認証部33によって検出し、認証する（ステップS6）。認証処理において、ワンタイムパスワードと個別IDとのうち、どちらか一方でも一致しない場合、エラーとなる。

【0020】一方、認証処理において、ワンタイムパス

ワードと個別IDとが一致する場合、利用者管理端末3は、このワンタイムパスワードと個別IDとが一致した利用者の個人情報の一部（例えば、住所と氏名）とを認証用利用者管理データベース32から読みだし、読み出した個人情報の一部と書類発行許可情報とを発行端末4に送信する（ステップS7）。

【0021】発行端末4は、利用者管理端末3から個人情報の一部と書類発行許可情報を受信すると、表示部に必要書類を選択するためのサービス選択画面の表示を行う。そして、利用者によって、サービス選択画面の中から「住民票」の項目が指定され、「住民票」を発行する料金が発行端末4に投入されると（ステップS8）、発行端末4の制御部41は、「住民票」を指定する情報と個人情報の一部と識別IDを発行させるためのコマンドとを発行物情報管理装置5に専用線11を介して送信する（ステップS9）。

【0022】発行物情報管理装置5は、発行端末4から「住民票」を指定する情報と個人情報の一部と識別IDを発行させるためのコマンドとを受信すると、「住民票」を指定する情報と個人情報の一部とに対応する利用者個人に関する情報を読み出し、読み出した利用者個人に関する情報に基づいて住民票を発行するための発行データを生成する。そして、発行物情報管理装置5は、識別IDを発行し、発行した識別IDと発行データとを発行端末4に送信する（ステップS10）。さらに、発行物情報管理装置5は、識別IDを書類発行用個人情報データベース51に記憶するとともに、利用者管理端末3に識別ID個人情報の一部とを通知する。発行端末4は、発行物情報管理装置5から送信される発行データを受信すると、受信した発行データに基づき、印刷部42によって住民票を印刷し、発行する（ステップS11）。利用者管理端末3は、発行物情報管理装置5から送信された個人情報の一部に対応するユーザIDに関連づけて、通知された識別IDを認証用利用者管理データベース32に記憶する。

【0023】以上説明した実施形態によれば、ステップS3において、ワンタイムパスワードを送信する場合に、ワンタイムパスワードの送信先の電子メールアドレスを利用者に入力させるのではなく、ステップS1において送信されるユーザIDとパスワードに対応する電子メールアドレスを認証用利用者管理データベース32から読み出し、読み出した電子メールアドレスを送信先としてワンタイムパスワードを送信するようにした。これにより、携帯電話1以外（例えば、パーソナルコンピュータ）からのアクセスを防止するとともに、ワンタイムパスワードを発行先である携帯電話1に確実に送信することができる。

【0024】また、上述の実施形態によれば、発行端末4と発行物情報管理装置5とを専用線11を介して接続するようにしたので、外部からの不正な侵入を低減させ

ることができる。また、上述の実施形態によれば、ネットワーク 2 に公式サイト網を適用することにより、携帯電話 1 の個別 ID に基づいて、アクセスしてきた携帯電話 1 の判別を容易に行うことができる。すなわち、公式サイト網を利用することにより、携帯電話 1 の通信サービス契約時に通信業者によって利用者が認証された後に付与される個別 ID が電子メールの送信時に利用者管理端末 3 に通知されるため、アクセスしてきた携帯電話 1 の所有者等の人物を特定することができる。また、特定の端末からのアクセスのみ受け付けるように制限することができ、これにより、パーソナルコンピュータ等比べて機能が限られた携帯電話からしかアクセスする事ができない。従って、公式サイト網を利用することにより、ハッキング等の不正行為を低減させることができる。

【0025】また、上述の実施形態によれば、情報発行システム側において、人手を介さずに発行処理を行うことができ、利用時間に制限を持たせることなく、24 時間対応のシステムの実現が可能であり、行政サービスの向上を図ることができる。また、上述の実施形態によれば、発行端末 4 が置いてある場所（コンビニエンスストアや駅など）一ヶ所に行くだけで複数の自治体から発行される公的書類もすべて手にすることも可能である。

【0026】利用者本人が発行端末 4 の側で発行操作を行うことにより、発行された印刷物をすぐに受け取ることができるとともに、第 3 者を介さずに印刷物を受け取ることができるので、発行された印刷物を利用者が受け取る前に盗難される場合を低減させることができる。

【0027】なお、以上説明した実施形態において、ワンタイムパスワードに有効期限を設けておき、有効期限が経過したワンタイムパスワードを認証用利用者管理データベース 3 上から削除するようにしてもよい。これにより、ワンタイムパスワードが悪用され不正なアクセスがなされることを低減させることができる。また、発行物の真偽を確認する必要がある場合は、真偽を確認する対象となる発行物が発行物情報管理装置 5 において発行されたか否かについて、書類発行用個人情報データベース 5 1 に識別 ID が記録されているか否かを確認することによって行われる。これにより、発行物の偽造などを発見することに利用でき、セキュリティの向上を図ることができる。また、利用者管理端末 3 の認証用利用者管理データベース 3 2 に記憶されている識別 ID を利用して、発行物の真偽を確認するようにしてもよい。

【0028】また、上述の実施形態においては、発行端末 4 によって公的証明書（住民票）を発行する場合について説明したが、発行端末 4 が発行する発行物は、公的証明書に限られるものではない。すなわち、書類発行用個人情報データベース 5 1 に記憶される情報は、利用者個人に関する情報に限られるものではなく、利用者に提供可能な情報であればよい。例えば、画像や、航空チケ

ット、コンサートチケット等の有償チケット等の情報等がある。

【0029】また、上述した実施形態において、携帯電話 1 から発行端末 4 にワンタイムパスワードを送信する場合に、電子メールを利用した場合について説明したが、ワンタイムパスワードを送信することができるものであれば、電子メール以外を用いるようにしてもよい。例えば、近距離無線通信（赤外線、BLUETOOTH 等）を利用してワンタイムパスワードを送信するようにしてもよい。また、携帯電話 1 と発行端末 4 とを接続コネクタ等を用いてワンタイムパスワードを送信するようにしてもよい。

【0030】また、上述した実施形態において、携帯電話 1 として、例えば、パームトップ・コンピュータ、ウェアラブル・コンピュータ等の携帯情報端末を適用するようにしてもよい。また、携帯情報端末または携帯電話 1 にユーザの情報が記録可能かつ取り外し可能な IC チップ等の記録媒体が搭載される場合、この記録媒体を携帯情報端末あるいは携帯電話 1 から取り出し、発行端末 4 に接続し、発行端末 4 によってこの記録媒体に記憶されたユーザの情報を読み出して認証を行った後、ワンタイムパスワード発行処理を行うようにしてもよい。

【0031】また、上述の実施形態において、利用者管理端末 3 においてパスワード等の認証する場合において、複数回（例えば、3 回）の認証失敗で該当ユーザ ID をロックする機能を設け、携帯電話 1 の盗難・窃盗による不正使用を防止するようにしてもよい。

【0032】また、図 1 におけるワンタイムパスワード発行部 3 1、認証部 3 3、制御部 4 1、印刷部 4 2 の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより情報の発行管理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、OS や周辺機器等のハードウェアを含むものとする。

【0033】また、「コンピュータシステム」は、WWW システムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ROM、CD-ROM 等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良



く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

【0034】以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【0035】

【発明の効果】以上説明したように、この発明によれば、携帯電話から送信される認証情報と識別情報とに基づいて認証処理を行い、認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを携帯電話に発行し、発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて一時記憶し、発行端末から送信される識別情報とワンタイムパスワードとを受信し、一時記憶された情報に基づいて認証処理を行い、認証が成立した場合に情報の発行を許可するようにした。これにより、セキュリティを向上させるとともに、必要な情報を簡単に取り寄せて発行することができる。

【0036】利用者は、情報の発行依頼を行う場合に、携帯電話から発行依頼を行うことができるので、コンピュータを利用する場合に比べて簡単に情報の発行を行うことができる。また、この発明によれば、発行毎に異な

るワンタイムパスワードを発行するようにしたので、さらにセキュリティを向上させることができる効果が得られる。

【0037】また、発行された証明書に対して識別IDを設けるようにしたので、発行された証明書の真偽を識別IDを利用して確認することも可能であり、セキュリティの向上を図ることができる効果が得られる。

【図面の簡単な説明】

【図1】 この発明の一実施形態による情報発行システムの構成を示す概略ブロック図である。

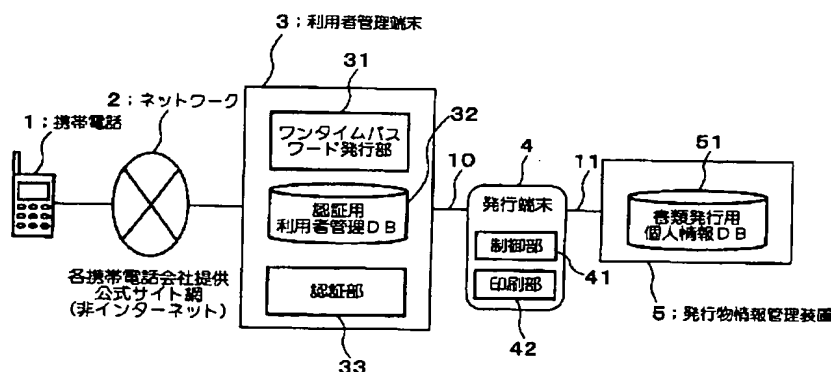
【図2】 認証用利用者管理データベース3に記憶される利用者管理情報を説明するための図面である。

【図3】 図1の構成における情報発行システムの動作を説明するための説明図である。

【符号の説明】

- |                   |                    |
|-------------------|--------------------|
| 1 携帯電話            | 3 利用者管理端末          |
| 4 発行端末            | 5 発行物情報管理装置        |
| 31 ワンタイムパスワード発行部  |                    |
| 32 認証用利用者管理データベース |                    |
| 33 認証部            | 41 制御部             |
| 42 印刷部            | 51 書類発行用個人情報データベース |

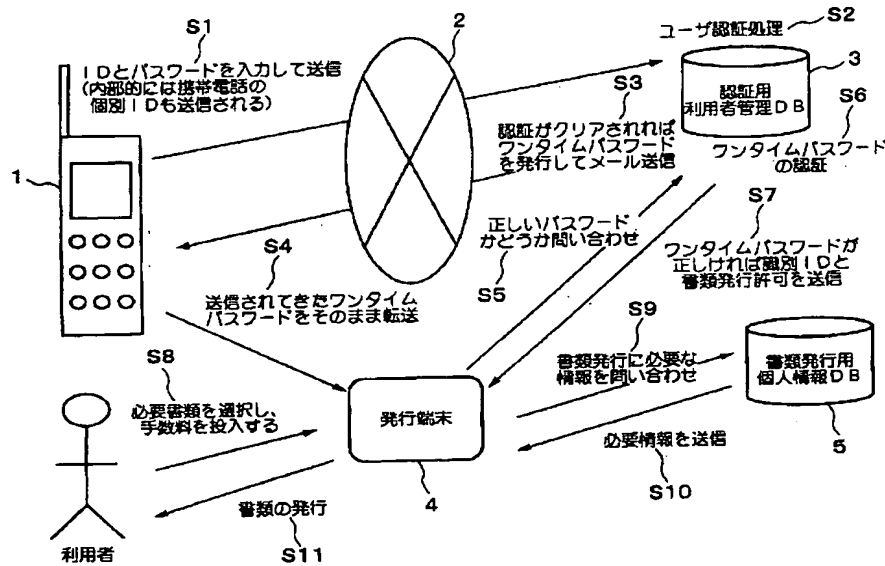
【図1】



【図2】

ユーザID	パスワード	個人情報	個別ID	メールアドレス	識別ID	フuntimeパスワード
U1D001	12345678	東京都...〇〇一郎	ABC0001	XX@△△.com	XYZ748	951183121
⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図3】



フロントページの続き

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
H 0 4 L 9/32		H 0 4 M 11/00	3 0 2
H 0 4 M 11/00	3 0 2	H 0 4 B 7/26	1 0 9 S
H 0 4 Q 7/38		H 0 4 L 9/00	6 7 3 A

Fターム(参考) 5B085 AA08 AE01 BA07 BE07 BG04  
BG07  
5J104 AA07 KA01 KA21 NA05 PA02  
PA07  
5K067 AA21 BB04 BB21 DD17 DD23  
EE02 EE10 HH22 HH23 HH24  
5K101 LL12 MM07 NN21 PP04

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**